Valeriana Gomes Roncero
roncero@cbpf.br

Marcelo Portes de Albuquerque
marcelo@cbpf.br

Márcio Portes de Albuquerque
mpa@cbpf.br

Monitoramento do Protocolo RTSP (Real Time Streaming Protocol) utilizando NTop (Network Top)

Resumo

Esta nota técnica tem o intuito de explicar como foi acrescentado ao aplicativo de monitoramento de tráfego da rede (NTop) uma análise do Real Time Streaming Protocol (RTSP). O RealPlayer, da empresa RealNetworks, é o software utilizado na Internet para transferir mídias de áudio e vídeo utilizando o protocolo RTSP. Neste projeto é utilizado o sistema operacional Linux para rodar o NTop, como também para a modificação e teste. O NTop (Network Top) é um aplicativo gratuito que permite o monitoramento da atividade da rede.

ÍNDICE DE TEXTO

Introdução

A análise de tráfego de rede tem sido considerada uma atividade importante desde o surgimento das redes. Os administradores devem gerenciar o tráfego de rede por várias razões, incluindo a detecção de sobrecarga na rede e/ou planejamento de expansão da rede.

Neste projeto são apresentados aspectos teóricos e práticos de uma atividade de monitoramento relacionada à medição do tráfego de rede do CBPF – Centro Brasileiro de Pesquisas Físicas. Esta medição e apresentação dos resultados obtidos são exibidas através de um navegador. Através do resultado é possível diagnosticar problemas que afetem o desempenho das diversas sub-redes que compõem a rede do CBPF.

A rede local do CBPF tem aproximadamente 800 equipamentos ligados em rede, e pertence à classe B. O domínio *cbpf.br* é representado pelo seguinte endereço 152.84.X.Y, sendo que, o X representa a sub-rede e o Y representa os *hosts*. O endereço 152.84.X.0 representa o IP da interface de rede, 152.84.X.1 representa o endereço do *gateway* e o 152.84.X.255 representa o endereço de *broadcast*. A rede local está dividida em 6 sub-redes: 152.84.250.0 (Administração), 152.84.253.0 e 152.84.50.0 (CAT), 152.84.100.0 (LAFEX), 152.84.10.0 (rede utilizada para testes) e 152.84.252.0 (outros departamentos).

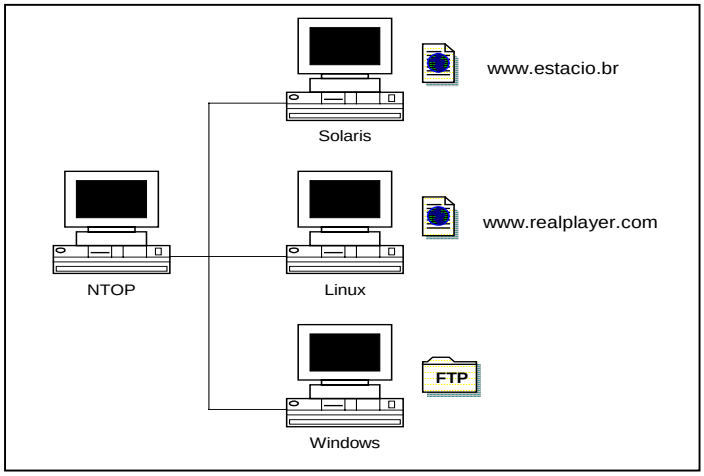

Figura 01 – NTop – Colentando dados de uma rede.

Neste trabalho são utilizados recursos computacionais com PC's /Linux, e o pacote de software de livre utilização denominado *NTop*. O *NTop* provê análise e estatísticas em tempo real, nos permitindo colher dados de utilização do segmento de rede, erros de pacotes e informações específicas de cada estação de trabalho. Com a finalização da coleta de dados sobre o tráfego do CBPF, será feita uma análise dos resultados obtidos. Pode-se observar na Figura 01 a funcionalidade do NTop.

O objetivo deste projeto é acrescentar ao software gratuito de monitoramento de tráfego da rede (NTop) a análise do protocolo RTSP (Real Time Streaming Protocol). Este protocolo é utilizado pelo software RealPlayer para transferir mídias de áudio e vídeo pela Internet. Tanto o NTop quanto o RealPlayer são executados no sistema operacional Linux.

Esta documentação está dividida em 5 capítulos: Capítulo 1 – Ferramentas de Monitoramento, Capítulo 2 – NTop – NetworkTop, Capítulo 3 – Real Time Streaming Protocol (RTSP), Capítulo 4 – Utilizando o Ntop, e Capítulo 5 - Adicionando o Protocolo RTSP ao NTop. No Capítulo 1 serão descritas algumas ferramentas de monitoração. No Capítulo 2 será descrito como é o funcionamento do NTop e algumas características do mesmo. O Capítulo 3 explica o funcionamento do protocolo RTSP. No Capítulo 4 será analisada as informações exibidas pelo NTop em uma coleta de dados. E para finalizar o Capítulo 5 descreve a alteração do código do NTop.

Capítulo 1 – Ferramentas de Monitoramento

1.1 Introdução

Neste capítulo serão demonstradas algumas ferramentas de análise de tráfego de rede.

1.2 Ferramentas

- Ethereal [3]
  O Ethereal é um analisador gráfico de protocolos de rede para ambientes Unix e Windows. Ele permite o exame dos dados trafegados na rede ou de registros de monitoração armazenados em disco. Neste último caso, possibilita percorrer os dados, visualizando informações de vários níveis para cada pacote.

- EtherApe [2]
  EtherApe é um monitor de rede gráfico para Unix. Com os modos Ethernet, IP e TCP, ele mostra a atividade da rede graficamente. As estações são representadas por pontos e o enlace entre eles por linhas que variam de espessura de acordo com o protocolo.

- IPTraf [5]
  O IPTraf é um utilitário de modo texto para levantamento de estatísticas de rede para Linux. Ele agrupa uma série de informações como o total de pacotes e *bytes* trafegados pela rede, indicadores de atividade, detalhamento do tráfego TCP e UDP, e total de pacotes e *bytes* trafegados pela estação de trabalho local.

- KNetDump [6]
  O KnetDump é uma ferramenta para analisar e visualizar os protocolos básicos do modelo OSI, camadas de 1 a 4. Tem fim didático, mostra os pacotes e o seu tráfego em diagramas semelhantes aos usados nos livros de redes. Oferece quatro visões diferentes: O KOSIView mostra as diferentes camadas do modelo OSI; o KTrafficView exibe as conexões de rede; o KHeaderView mostra cada pacote recebido pela rede em uma estrutura de cabeçalhos e o KChartView mostra as conexões TCP entre duas estações.

- KSniffer [7]
  O KSniffer é uma versão gráfica do IPTraf, que inclui outras funcionalidades como gráficos de uso da rede em geral ou mesmo de protocolos em vários níveis da pilha TCP/IP.

- KSnuffle [8]
  O KSnuffle é um investigador de pacotes (que será explicado no capítulo 2) para o ambiente KDE. Ele permite a investigação remota, podendo exibir vários monitores concorrentemente. Assim como o Ethereal, o KSnuffle permite a reconstrução de uma conexão a partir da escolha de um pacote que faz parte da mesma.

- NTop [11]
  O NTop é um aplicativo que permite o monitoramento da atividade da rede, de forma similar à ferramenta *Top* do Unix, que informa quais são os processos que a CPU utiliza e o desempenho dela. Possui também uma interface HTML com uma série de estatísticas e gráficos.

- TCPDstat [13]
  O TCPDstat provê um sumário de informações de um arquivo gerado pelo TCPDump. O TCPDstat lê o arquivo do TCPDump usando a biblioteca *pcap* (que será explicada no Capítulo 2) e imprime as estatísticas do registro de monitoração. A sua saída inclui o número de pacotes, taxa média de transmissão e o seu desvio padrão, o número de pares únicos de endereços fonte e destino, e o número de pacotes e de *bytes* por protocolo. Ele também oferece dados úteis para se encontrar uma anomalia no registro de monitoração. Por exemplo, o tráfego intenso de ICMP ou entre um par de endereços específicos, pode ser sinal de algum tipo de ataque de negação de serviço (DoS).

- TCPDump [14]
  O TCPDump é um programa que coloca a interface de rede em modo promíscuo, ou seja, aceitando todos os pacotes que trafegam pela rede. O TCPDump possui um mecanismo poderoso de filtragem de pacotes, de modo a armazenar apenas os dados que sejam de interesse.

- TCPFlow [15]
  O TCPFlow é um programa de captura os dados transmitidos em uma conexão TCP e os armazena em uma forma conveniente para análise, reconstruindo as seqüências de pacotes. Ele entende e reconstrói seqüências de dados de forma independente de retransmissões ou do envio fora de ordem. É baseado na biblioteca *pcap* e, portanto suporta as mesmas expressões de filtragem de programas como o TCPDump, como foi mencionado anteriormente.

- TCPSlice [16]
  TCPSlice é um programa para extração de partes de arquivos de registro gerados pelo TCPDump. Ele também pode ser usado para reunir vários destes arquivos. Sua função é copiar para a saída padrão todos os pacotes que estejam dentro de um intervalo de tempo especificado.

- TCPStat [17]
  TCPStat relata certas estatísticas de rede de forma semelhante ao que o vmstat faz para estatísticas de sistema. Tais estatísticas incluem a banda que está sendo utilizada, o número e o tamanho médio dos pacotes por intervalos determinados de tempo. O TCPStat coleta estatísticas pela leitura de um arquivo ou pelo monitoramento direto da interface de rede. É altamente configurável, sua página principal detalha mais de 15 diferentes tipos de estatísticas disponíveis.

- TCPTrace [18]
  O TCPTrace é uma ferramenta de análise de conexões TCP em arquivos de registro. Para cada conexão ele detalha o tempo gasto, o número de *bytes*/segmentos (unidades de dados TCP) enviados e recebidos, retransmissões e outros parâmetros com tempo de ida e volta do pacote (até chegar o reconhecimento), anúncios de janelas de recepção e vazão. O nível de detalhe da saída produzida pelo programa pode ser variado para atender a diferentes necessidades.

1.3 Conclusão

Foram citados somente alguns softwares, mas existem mais softwares disponíveis mundialmente. Todos estes softwares capturam e analisam os pacotes transmitidos na rede, gerando vários resultados, como estatísticas de rede, gráficos e tabelas de comparações.

A ferramenta NTop foi desenvolvida para resolver problemas de desempenho do *backbone* da rede do campus da Universidade de Pisa, na Itália. Os desenvolvedores precisaram de uma ferramenta simples capaz de informar rapidamente quais são as estações que estão usando a maioria dos recursos disponíveis atualmente da rede.

Em virtude dessas características apresentadas, a ferramenta NTop foi escolhida para desenvolver este trabalho. No Capítulo seguinte serão detalhadas as características desta ferramenta.

Capítulo 2 – NTop – Network Top

2.1 Introdução

A tarefa de administração de rede está ficando bastante complexa, devido ao número crescente de computadores em rede, rodando diferentes sistemas operacionais e falando vários protocolos de comunicação. A maioria das ferramentas de monitoramento e diagnóstico da rede, como *ping* e *traceroute*, é satisfatória para resolverem problemas simples de diagnóstico e monitoração. Os complexos problemas de rede precisam ser freqüentemente endereçados usando ferramentas de administração bastante caras ou detectores disponíveis em empresas de médio-porte.

A ferramenta NTop é um programa de código-fonte aberto baseado no monitoramento da utilização da rede que permite aos usuários localizarem atividades pertinentes de rede, incluindo utilização da rede, estabelecimento de conexões, o uso de protocolos de rede e classificação do tráfego.

Na era da *Internet*, os usuários de estações precisam ter acesso as poderosas ferramentas de monitoramento de rede capazes de dar informação sobre a rede, tais como:

- Desempenho da rede local.
- A estação que está utilizando a maioria da largura da banda da rede disponível.
- As estações que estão diminuindo atualmente o desempenho do servidor local de NFS.
- A porcentagem de largura da banda atualmente utilizada por uma estação.
- Os pares de comunicação e a quantidade de tráfego de rede produzido por cada um dos processos que estão rodando em uma estação.
- As estações que produzem tráfego *Multicast*.

2.2 Conhecendo o NTop

O NTop é um software de aplicação com o código-fonte aberto desenvolvido na linguagem C e disponível gratuitamente.

As metas principais desenvolvidas para o NTop são:

- portabilidade para as plataformas Unix e não-Unix (por exemplo, versões do Windows de 32 bits.);
- simples e eficiente aplicação do *kernel* com baixo uso de recursos (memória e CPU);
- exigências mínimas (sistema operacional simples) mas capazes de explorar as características da plataforma presentes (por exemplo, linhas de execução, ou *threads*, do *kernel*);
- habilidade de exibir os dados no modo interativo ou *web*;
- a saída da análise de rede é rica em conteúdo e fácil de ler.

A arquitetura do NTop é mostrada na figura seguinte.

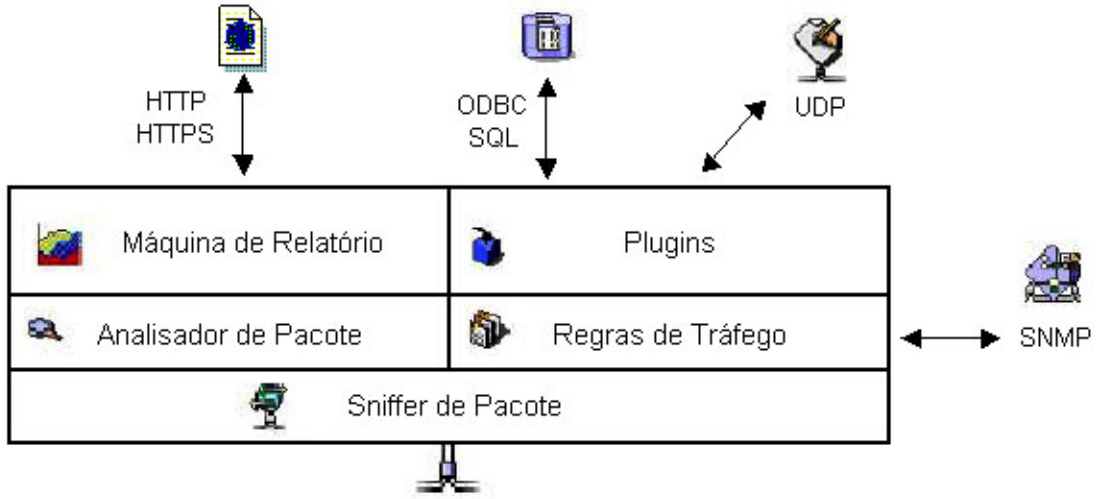

Figura 02 – Arquitetura do NTop

O investigador de pacote coleta os pacotes da rede e então passa para o analisador de pacote para o processamento. Sempre que a informação de tráfego tem que ser exibida, a máquina de relatório apresenta adequadamente a informação solicitada. Cada um dos campos citado será descrito a seguir.

2.2.1 Investigador de Pacote

O investigador (*sniffer*) é um programa que monitora e analisa o tráfego de rede, detectando a sobrecarga da rede e problemas. Utilizando esta informação, o administrador da rede pode manter o tráfego fluindo eficientemente.

O investigador de pacote é o componente do NTop que potencialmente tem mais resultados portáveis. De fato, ao contrário de outras facilidades como linhas de comandos, não há uma biblioteca portável para capturar pacotes. No Unix a biblioteca Libpcap provê a portabilidade e a unificação da interface de captura de pacotes, considerando que outros sistemas operacionais provêem a sua própria facilidade de captura. Devido ao bom desenvolvimento do Libpcap e de sua interface relativamente portável, os desenvolvedores decidiram usar o Libpcap como interface de captura unificada e então agrupar as bibliotecas de captura de pacote da plataforma utilizada (por exemplo, NDIS [10] em Win32). A vantagem é que o código do NTop é único, considerando que o código específico da plataforma utilizada é limitado a um arquivo.

O investigador de pacote suporta diferentes tipos de interface de rede incluindo interfaces para PPP, Ethernet e Token Ring, e permite filtrar pacotes capturados antes de serem processados pelo analisador. O filtro de pacotes é baseado na facilidade do filtro BSD Packet Filter [1] do Libpcap. Os filtros são especificados utilizando expressões simples as quais são aceitas pelo TCPDump.

As bibliotecas de captura de pacote têm pequenos *buffers* internos que impedem as aplicações de serem conduzidas para a sobrecarga de tráfego. Para superar este problema que conseqüentemente reduz a perda de pacote, o NTop armazena os pacotes capturados em um *buffer*. Permitindo ao analisador de pacotes ser desacoplado do investigador de pacote e não perder pacotes devido à sobrecarga de tráfego.

2.2.2 Analisador de Pacote

O analisador de pacote processa um pacote de cada vez. Os cabeçalhos dos pacotes são analisados de acordo com a interface de rede que está sendo usada, porque os cabeçalhos são diferentes dependendo da interface de rede (por exemplo, o cabeçalho do Token Ring é diferente do cabeçalho da Ethernet).

As informações sobre as estações são armazenadas em uma tabela *hash* cuja chave é o endereço de hardware de 48 bits (MAC – Controle de Acesso ao Meio) que garante sua singularidade e permite diferentes protocolos de rede que não rodam sobre IP sejam controlados. Cada entrada contém vários contadores que armazena a quantidade de dados enviados e recebidos pela estação, ordenados de acordo com os protocolos de rede suportados. Para cada pacote, a entrada *hash* corresponde a fonte e destino do pacote é atualizada ou criada, se não estiver presente. Porque não é possível predizer o número de diferentes estações cujos pacotes serão controlados através do NTop, seria quase impossível ter uma grande tabela *hash* suficiente o bastante para acomodar todas as possíveis estações. Quando é necessário (por exemplo, periodicamente ou se há nenhuma entrada abandonada) o NTop elimina a tabela de estações para evitar uma descarga em toda a memória disponível e a criação de grandes tabelas que diminuem toda o desempenho. Entradas eliminadas correspondem a estações que não têm dados enviados e recebidos por um longo período de tempo. Isto garante que a utilização de memória pelo NTop não cresce indefinidamente e o tempo de processamento do pacote não aumenta linearmente com o número de estações ativas. Se o pacote recebido for um pacote não-IP, os contadores de entrada de protocolo são atualizados e o pacote é descartado. Se o pacote recebido for um pacote IP, então o processamento é executado.

O armazenamento é executado de duas formas. O primeiro nível de armazenamento é baseado no GNU gdbm [04], que é um conjunto de rotinas de acesso à banco de dados.

Figura 03 – Armazenamento do NTop.

O segundo nível de armazenamento é implementado utilizando o banco de dados SQL. O NTop captura as informações locais semipersistentes, como endereço IP (mapeando numericamente ou simbolicamente o endereço IP), e um sistema operacional de uma estação remota. Os eventos da rede (por exemplo, sessões TCP), desempenho dos dados e outras informações relevantes são armazenadas permanentemente no banco de dados. O armazenamento acontece periodicamente ou quando o coletor de lixo tem que eliminar alguns dados.

O NTop comunica-se com o banco de dados por meio de uma aplicação cliente. Assim, o cliente dialoga com o NTop via UDP e comunica-se com o banco de dados que usa ODBC (Open DataBase Connectivity Protocol). Sempre que algumas informações de rede precisam ser armazenadas no banco de dados, o NTop envia para o cliente um ou mais pacotes UDP que contêm declarações válidas de SQL. O

cliente, atualmente implementado em Perl e Java, recebe os pacotes e executa a declaração no banco de dados local pelo Perl DBI (DataBase Interface) ou Java JDBC (Java DataBase Connectivity) dependendo da linguagem implementada.

A entrada de uma estação é mostrada abaixo contendo um contador para cada um dos protocolos IP especificados do usuário.

Entrada da tabela *hash* de uma estação.	Contador de Tráfego de Protocolo
	Contador de Tráfego IP
	Estatísticas das Conexões TCP/UDP
	Lista das Conexões TCP Ativas
	Lista de Pares

Tabela 1 – Entrada da tabela hash de uma estação.

Para cada pacote IP, o contador do protocolo é atualizado. Se o pacote for um fragmento IP, o NTop atualiza a informação, como, a porta de origem e destino da tabela *hash* de fragmentos. Sempre que o primeiro fragmento de pacote é encontrado, a informação sobre o fragmento é armazenada na tabela *hash* que utilizando o identificador do fragmento de pacote (*fragmentId*) como chave do *hash*. A informação sobre o fragmento é removida assim que o último fragmento é recebido. Porque poderia acontecer de que alguns pacotes (inclusive fragmentos) fossem descartados, a tabela de fragmento é periodicamente analisada e a informação desatualizada é eliminada disto.

A entrada da estação também contém uma lista (inicialmente vazia) das conexões TCP ativas da estação ntop. O NTop armazena o estado de cada conexão TCP analisando os *flags* de IP. Conseqüentemente se o pacote recebido é um pacote TCP, então a lista da conexão TCP da estação ntop também precisa ser atualizada.

Embora os contadores de tráfego da estação ntop possam ser usados para analisar o tráfego de rede, em alguns casos poderia ser necessário estudar um tráfego específico que flui por algumas estações. O NTop permite que os usuários possam escolher os fluxos de rede. Um fluxo de rede é um fluxo de pacotes que está relacionado a uma regra definida pelo usuário. As regras são especificadas utilizando expressões de BPF. O fluxo de rede do NTop pode ser utilizado para detalhar um tráfego de interesse particular. Os fluxos de rede podem ser muito úteis para depurar problemas de rede, agrupando dados estatísticos ou localizando um acesso suspeito para alguns recursos de rede especificados.

2.2.3 Máquina de Relatório

A versão atual do NTop pode ser inicializada de duas maneiras:

a. Modo interativo
   O NTop é executado em terminal e os usuários podem interagir, utilizando o teclado.
b. Modo *web*
   O NTop age como um servidor HTTP e permite aos usuários remotos analisarem as estatísticas de tráfego por meio de um navegador *web*.

O NTop foi projetado para ser independente da maneira de que os relatórios de tráfego são criados. A máquina de relatório contém dois emissores, um para o terminal e outro para o HTML. A independência do modo no qual os relatórios são criados é muito importante para garantir a evolução da aplicação. Na realidade, se uma nova linguagem como XML tem que ser implementada, somente a máquina de relatório precisa ser estendida considerando que o resto da aplicação permanece inalterado. Vale a pena notar que as informações e as estatísticas podem ser geradas utilizando os dados armazenados pelo NTop no banco de dados SQL.

2.3 Funções

Esta seção apresenta um completo detalhamento das funções principais do NTop: medidor de tráfego, monitoramento de tráfego, otimização e planejamento da rede, e detecção de violações na segurança da rede.

2.3.1 Medida de tráfego

A medida de tráfego consiste em medir a utilização de atividades relevantes do tráfego. O NTop observa a utilização da rede, gerando umas séries de estatísticas para cada estação numa subrede IP local e para uma subrede como um todo. A informação necessária é coletada pela estação ntop simplesmente observando o tráfego na rede. Este método não necessita dos requerimentos de processamentos dos nós operacionais da estação ntop. Todos os pacotes na subrede são capturados e associados com um par de emissor e receptor. Deste modo, é possível observar todas as atividades do tráfego de uma estação em particular.

A seguinte tabela informa as estatísticas globais de tráfego, inclusive:

DISTRIBUIÇÃO DO TRÁFEGO	Tráfego local (subrede), local versus remoto (subrede local/especificada externamente), remoto versus local.
DISTRIBUIÇÃO DE PACOTES	Número total de pacotes ordenados pelo tamanho de pacote, *unicast* versus *broadcast* versus *multicast* e tráfego IP versus não-IP.
LARGURA DA BANDA USADA	Atual, média e máxima utilização da largura de banda.
UTILIZAÇÃO E DISTRIBUIÇÃO DO PROTOCOLO	Distribuição do tráfego observado de acordo com o protocolo e par origem-destino (local versus remoto).
MATRIZ DE TRÁFEGO DA SUBREDE LOCAL	Tráfego monitorado entre cada par de estações em uma subrede.
FLUXO DE REDE	Estatísticas de tráfego para fluxos definidos pelo usuário (tráfego de interesse particular do usuário).

Tabela 2 – Estatísticas Globais registradas pelo NTop.

O NTop também exibe a informação registrada de cada estação conectada a uma rede *broadcast*:

DADOS ENVIADOS E RECEBIDOS	O total de tráfego (volume e pacotes) gerado ou recebido pela estação. Classificado de acordo com o protocolo da rede (IP, IPX, AppleTalk, etc.) e protocolo IP (FTP, HTTP, NFS, etc.).
LARGURA DE BANDA USADA	Atual, média e máxima utilização da largura de banda.
IP *MULTICAST*	Quantidade total de tráfego *multicast* gerado ou recebido pela estação.
HISTÓRICOS DAS SESSÕES TCP	Sessões TCP atualmente ativas estabelecidas ou aceitadas pela estação e estatísticas de tráfego associadas.
TRÁFEGO UDP	Quantidade total de tráfego UDP ordenado por porta.
SERVIÇOS TCP E UDP USADOS	Lista de serviços baseados em IP (por exemplo abrir e ativar portas) fornecida pela estação ntop com uma lista das últimas 5 estações que os utilizaram.
DISTRIBUIÇÃO DE TRÁFEGO	Tráfego local, tráfego local para remoto, tráfego remoto para local (estações locais são adicionadas na rede *broadcast*).
DISTRIBUIÇÃO DO TRÁFEGO IP	Tráfego UDP versus TCP, distribuição relativa de protocolos IP de acordo com o nome da estação.

Tabela 3 – Informação registrada pelo NTop para cada estação.

Além da informação fornecida acima, a versão atual permite que a instalação de *plug-ins* para prover estatísticas detalhadas sobre protocolos particulares que não estão presente na versão padrão. Exemplos destes são os *plug-ins* NFS e NetBIOS. O NTop também gerará estatísticas sobre a estação ntop, escutando os *sockets* abertos, dados enviados e recebidos, e pares contatados para cada processo.

2.3.2 Monitoramento de tráfego

O monitoramento de tráfego é a habilidade de identificar algumas situações aonde o tráfego da rede não obedece às políticas especificadas ou quando excede alguns limiares definidos. Em geral, os administradores de rede especificam políticas que aplicam ao comportamento de elementos que são transmitidos na rede gerenciada. Não obstante, é possível que algumas estações não obedeçam a política prescrita. Causas típicas de mau comportamento são relacionadas com a má configuração de sistemas operacionais, interfaces de rede, aplicações de software e outros.

O NTop provê suporte para detecção de alguns problemas de configuração de rede, como:

- Uso de endereços IP duplicados.
- Identificação de estações locais em "modo promíscuo".
- Má configuração das aplicações de software, por dados de tráfego do protocolo analisados.

- Detecção da má utilização do serviço, identificando estações que não utilizam os *proxies* especificados.
- Má utilização do protocolo, identificando estações que usam protocolos desnecessários.
- Identificação de rotas na subrede, detectando má configuração de estações de trabalho que agem como rotas.
- Utilização excessiva de largura da banda da rede.

2.3.3 Otimização e Planejamento de Rede

A configuração não otimizada de estações poderia influenciar negativamente o desempenho global de uma rede. O NTop permite ao administrador identificar fontes potenciais de uso de largura da banda improdutivas, particularmente o uso de protocolos desnecessários e problemas de roteamento não otimizados. Indiretamente, pela caracterização e distribuição do tráfego, é possível revisar políticas para a rede promover mais sabiamente o uso de largura da banda.

2.3.4 Detecção de Violações de Segurança de Rede

Em redes, a maioria dos ataques de segurança vêm da própria rede interna. Por esta razão, o NTop provê aos usuários o suporte para localizar ataques contínuos e identificar falhas potencias na segurança, como, IP *spoofing*, placas de rede em modo promíscuo, ataques de negação de serviço, cavalos de tróia (que usam portas conhecidas) e ataques *portscan.*

Quando uma violação de segurança ou uma má configuração de rede é identificada, o NTop oferece instalações para gerar alarmes para o operador de rede e executar ações específicas (quando aplicável) a fim de bloquear os ataques. Como também é possível armazenar informação de tráfego em um banco de dados, os registros podem ser usados para entender o ataque e prevenir ocorrências similares no futuro.

É importante notar que o NTop, como também outras ferramentas de monitoramento, poderia gerar ameaças de segurança se não fosse instalado e configurado corretamente. O acesso livre para a interface *web* do NTop permitirá a qualquer usuário com acesso a *web* ler toda a informação fornecida pelo NTop, adquirindo conhecimento sobre a rede. Isto não ocorreria caso o acesso fosse restrito. O administrador do NTop pode cadastrar os usuários para que eles tenham acesso a *web*, com os dados armazenados de forma encriptada em um banco de dados.

2.4 Funcionamento do NTop

2.4.1 Modo Interativo

Quando o NTop é executado no modo interativo utilizando o comando *INTop*, a informação de tráfego é exibida em uma janela de terminal como mostrado a seguir.

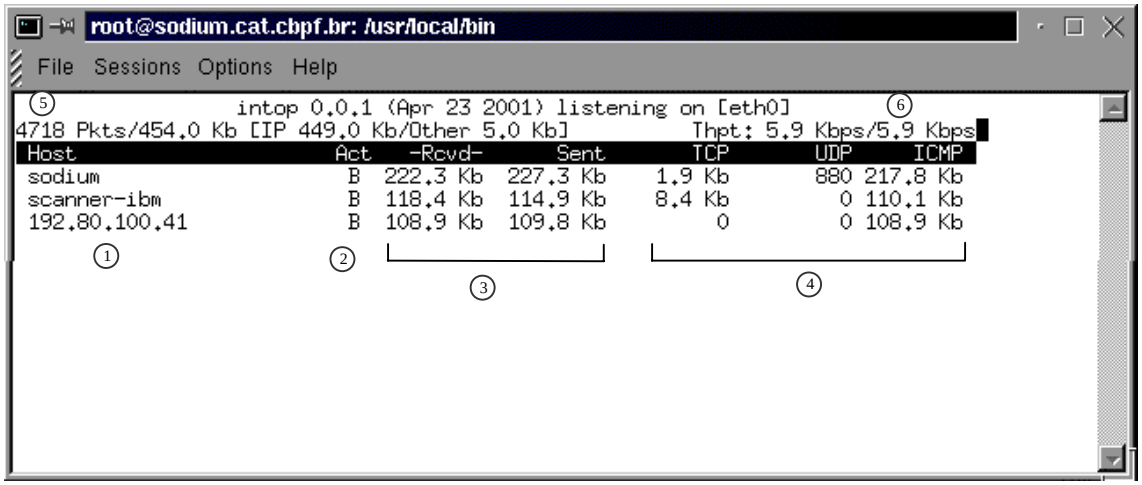

Figura 04 – NTop: Modo interativo

A coluna (1) contém a lista de estações que têm dados enviados e recebidos, a coluna (2) especifica o estado da estação (S=enviar, R=receber, B=enviar e receber, e I=ocioso). A coluna (3) contém o total de dados enviados e recebidos por cada estação, considerando que a coluna (4) é uma visão detalhada da coluna anterior. Os usuários podem alterar a ordem de listagem ou a exibição dos protocolos simplesmente apertando as chaves apropriadas. O terminal é periodicamente atualizado conforme a especificação feita pelo usuário. O item (5) indica o total de tráfego observado (pacotes e *bytes*) a partir da hora em que o NTop foi inicializado, considerando que o fluxo atual e máximo da rede é mostrado no item (6).

2.4.2 Modo *Web*

O NTop no modo interativo foi concebido como uma ferramenta de diagnóstico rápido de rede para usuários que precisam ter que verificar rapidamente para o atual tráfego de rede (por exemplo, quando a rede está lenta e é necessário achar quais são as estações que estão diminuindo o desempenho global). Ao invés disso, o modo web transformou o NTop em uma aplicação de administração baseada em web como mostrado na figura seguinte.

O modo *web* foi projetado, como uma aplicação que contém longas estatísticas com pausas sendo capaz de prover aos usuários uma visão detalhada das atividades atuais e passadas da rede. A interface do modo *web* foi selecionada, porque garante a independência do cliente e permite a múltiplos usuários o acesso de leitura dos resultados.

Para impedir aos usuários sem autorização acessarem os dados, como informação de tráfego, o NTop implementa o esquema HTTP padrão de proteção por senha. Os administradores podem especificar no nível do usuário quais informações podem ser apresentadas aos usuários remotos para evitar exposição de importantes informações para hackers potenciais, assim, permitindo somente as pessoas selecionadas terem acesso a todas as estatísticas de rede.

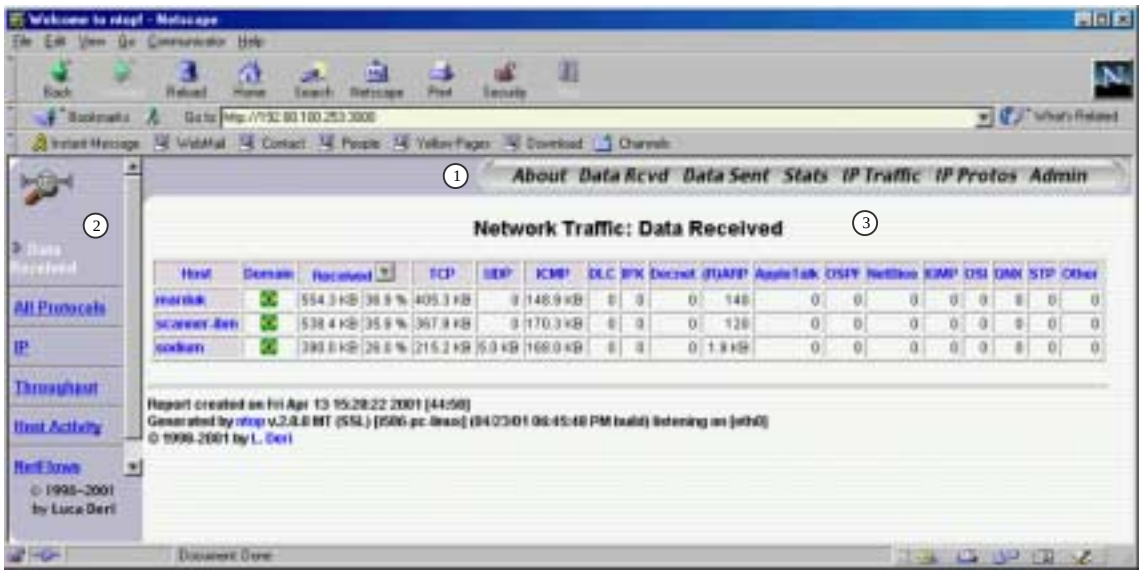

Figura 05 – NTop: Modo Web

Os usuários podem ser conectar diretamente ao NTop, o qual atua como servidor HTTP, pelo seu navegador *web*. A página de entrada é dividida em três quadros: o quadro (1) é o menu usado para navegar pela informação de tráfego. Cada um dos itens deste menu está especificado no quadro (2). E a informação sobre o tráfego é exibida no quadro (3). Todas as colunas de uma tabela são ordenadas simplesmente clicando com no nome da coluna. As páginas HTML são atualizadas automaticamente ou se o usuário solicitar.

Além das informações exibidas no modo interativo, o modo *web* contém estatísticas adicionais incluindo:

- IP *Multicast*
- Informação sobre a estação, como dados enviados e recebidos, pares conectados, sessões ativas de TCP, histórico das sessões TCP e UDP, serviços IP disponíveis ou utilizados, largura da banda atualmente em uso.
- Estatísticas de tráfego, como tráfego local (subrede), local versus remoto (fora de redes especificadas/locais), remoto versus local, estatísticas de pacote, nível de processamento da rede (atual, máximo, médio).
- Fluxo de sessões ativas de TCP.
- Distribuição de protocolos que rodam ou não sobre IP.
- Distribuição do tráfego observado de acordo com o protocolo e, origem e destino (local versus remoto).
- Matriz de tráfego da subrede.
- Fluxos da rede, com estatísticas de tráfego para cada fluxo definido de usuário.
- Utilização da rede local, com estatísticas detalhadas sobre sockets abertos, dados enviados/recebidos, e pares conectados para cada processo que está rodando na estação ntop.

O NTop utiliza uma ferramenta chamada lsof [9] para calcular a utilização da rede local. O lsof é utilizado na inicialização do NTop para adquirir a lista de portas IP abertas para cada um dos processos em execução. O NTop executa o lsof periodicamente ou sempre que uma estação remota envia ou recebe dados de uma porta local que não estava ativo quando o lsof foi executado pela última vez. A utilização do lsof é justificada pelo fato de que não há um modo portável para atualizar a lista de portas IP abertas para cada um dos processos em execução, e até mesmo se o NTop implementasse está funcionalidade, o NTop tem que periodicamente avaliar

o *kernel* porque não há um modo para a notificação de quando uma porta é aberta ou fechada.

2.4.3 Quando usar NTop?

O NTop pode ser usado para monitorar a rede quando alguns problemas surgirem ou somente para analisar o estado global da rede incluindo:

- Monitoramento de protocolo, determinando quais são os protocolos utilizados e identifica as estações que falam protocolos desnecessários. Por exemplo, o sistema operacional Windows instala por padrão protocolos como *NetBeui* e *IPX* enquanto a maioria das pessoas utilizam somente TCP/IP.
- Utilização dos serviços da rede, como os serviços DNS e NFS podem ser facilmente monitorados. Permitindo que os administradores de rede analisem o impacto de protocolos selecionados no desempenho global da rede e identifiquem aplicações (por exemplo, um servidor de FTP) que foram instaladas silenciosamente na rede sem autorização.
- Utilização da rede, permitindo o NTop identificar quais são as estações que estão utilizando a maioria dos recursos de rede, como também o gráfico de utilização da largura da banda na rede durante um determinado tempo.
- Segurança, as falhas de segurança, como *portscan*, negação de serviço e outros tipos de falhas, são localizadas pelo NTop, e uma vez armazenadas no banco de dados podem ser utilizadas para identificar as estações que violaram a segurança global da rede.

Em geral, o NTop reúne características às vezes presente em várias ferramentas que não são sempre fáceis de integrar.

2.4.4 Desempenho

O desempenho do NTop é bastante satisfatório basicamente por cinco razões:

- A performance do Libpcap (ou NDIS em Win32) é excelente;
- A quantidade de perda de pacote é muito baixa (se existir), porque os pacotes capturados são armazenados duas vezes, uma dentro do *kernel* e a outra no NTop;
- Ações de longo tempo de execução (por exemplo, resolução de endereçamento IP) são implementadas no modo assíncrono;
- O NTop gera várias linhas de comandos que previnem a interação do usuário (por exemplo, solicitação do usuário HTTP) de interferir na coleta de dados;
- O NTop faz uso extenso de tabelas *hash* cujos índices são fáceis de computar durante a rápida recuperação de informação devido à natureza de endereços de rede (por exemplo, eles são únicos e no formato numérico de 32/48 bits).

Em geral, o desempenho do NTop é influenciado pelos outros processos correntes porque algumas aplicações “gananciosas” de CPU podem utilizar todos os ciclos da CPU durante alguns segundos causando a perda de pacotes.

O desempenho do NTop também é influenciado se forem definidos mais fluxos de rede, pois mais tempo de processamento será necessário, podendo causar a perda de alguns pacotes. Dependendo do modo no qual o NTop trabalha, se um pacote se perde podem surgir grandes problemas. Suponhamos que foi perdido o primeiro

fragmento de um pacote TCP que contém o *flag FIN*, que indica o encerramento da conexão TCP. Neste caso dois problemas existem:

- a entrada do fragmento para o pacote não é criada, conseqüentemente os pacotes seguintes não podem ser controlados corretamente;
- o NTop não sabe que um par pretende fechar a conexão TCP.

Para resolver os problemas mencionados acima, o NTop implementa intervalos internos e a coleta periódica de lixo para eliminar os dados antigos e refletir sobre o estado de conexões ativas. Por exemplo, se não houver dado fluindo em uma conexão por um longo período de tempo, então a conexão poderia ter sido fechada. Neste caso, o NTop assume que a conexão foi fechada e então a entrada de conexão é eliminada. Permite-se desta forma que o NTop se recupere quando alguns pacotes se perderem e não seja impedido de prosseguir esperando por algum pacote perdido chegar.

2.5 Conclusão

Este capítulo descreveu como o NTop pode ser utilizado para medida e monitoramento de tráfego. As características mais importantes deste software são: um servidor HTTP embutido, suporte a vários tipos de enlaces de rede, pouca utilização da CPU, portabilidade para várias plataformas, armazenamento das informações de tráfego em um banco de dados SQL, e integração com várias ferramentas de rede. Esta integração com as ferramentas de rede tornam o NTop adequado para aqueles que querem analisar o tráfego da rede sem tem que pagar por ferramentas caras que às vezes têm limite de escopo e falta de algumas características oferecidas pelo NTop.

Capítulo 3 – Real Time Streaming Protocol (RTSP)

3.1 Introdução

Neste capítulo será abordado como funciona o protocolo RTSP utilizado pela tecnologia da RealNetworks [12] para transmissão de *streams*. Internamente, o RTSP utiliza os protocolos UDP ou TCP. Um link para um conteúdo de media da Real, tem o formato *rtsp://nome_do_servidor/arquivo.rm*.

3.2 Real Time Streaming Protocol (RTSP)

O RTSP é um protocolo a nível de aplicação para controle na transferência de dados com propriedades de tempo real. RTSP torna possível a transferência, sob demanda, de dados em tempo real como áudio e vídeo. Ele serve para estabelecer e controlar um único ou vários *streams* sincronizados de mídias contínuas pertencentes a uma apresentação.

O conjunto de *streams* a ser controlado é definido por uma descrição de apresentação, normalmente um arquivo, que pode ser obtido por um cliente usando HTTP ou outro meio como e-mail; e, pode não necessariamente estar armazenado em um servidor de mídia.

Uma descrição de apresentação contém informações sobre um ou mais *streams* que compõe a apresentação, como endereços de rede e informações sobre o conteúdo da apresentação (por exemplo, assunto, e-mail do responsável pela sessão, tempo da apresentação), além de parâmetros que tornam possível ao cliente escolher a combinação mais apropriada das mídias. Na descrição da apresentação, cada *stream* é individualmente identificado por uma URL RTSP, a qual aponta para um servidor de mídia que trata aquele *stream* particular e dá um nome ao *stream* armazenado naquele servidor. Vários *streams* (áudio e vídeo) podem ser localizados em servidores diferentes para compartilhamento de carga. Além disso, a descrição da apresentação também descreve quais métodos de transporte o servidor é capaz de oferecer. Vários modos de operação são utilizados como *unicast* e *multicas*t. Em relação ao funcionamento de RTSP, não existe a noção de uma conexão RTSP; ao invés disso, um servidor mantém uma sessão indicada por um identificador. Uma sessão RTSP não está ligada à uma conexão a nível de transporte como acontece numa conexão TCP. Durante uma sessão RTSP, um cliente RTSP pode abrir e fechar conexões de transporte para o servidor emitir requisições RTSP, sendo que, normalmente, o controle RTSP pode acontecer em uma conexão TCP enquanto o fluxo de dados via UDP ou RTP; mas, a operação de RTSP não depende do mecanismo de transporte utilizado para o transporte das mídias contínuas.

O protocolo suporta as seguintes operações: recuperação de mídia de um servidor de mídia, convite de um servidor de mídia para uma conferência (apresentação ou registro de um, ou um subconjunto de mídias da conferência), e adição de mídias a uma apresentação existente.

Como exemplo da utilização de RTSP temos mídia sob demanda (Figura 5). Em mídia sob demanda, um cliente requisita um filme de um servidor de áudio (áudio.exemplo.com) e um servidor de vídeo (vídeo.exemplo.com). A descrição da

mídia é armazenada em um servidor *Web*. O cliente estabelece uma conexão com o servidor Web solicitando o arquivo de descrição da apresentação. O servidor Web responde com OK e mais informações (tipo de conteúdo a ser apresentado, o endereço onde áudio e vídeo encontram-se). Logo depois, o cliente envia um comando para o servidor de áudio e para o servidor de vídeo pedindo para iniciar uma sessão (método SETUP) e em seguida para inicializar a representação de áudio e vídeo (método PLAY). Os servidores enviam respostas de OK e em seguida enviam através de RTP ou outro protocolo de transporte áudio e vídeo ao cliente. Cabe ressaltar que RTCP faz-se presente aqui fornecendo informações de sincronização para o cliente e informações de perda de pacotes para o servidor, entre outras. Por fim, o cliente solicita aos servidores para liberar recursos através do comando TEARDOWN encerrando a sessão RTSP com uma resposta de OK dos servidores.

Já existem implementações de RTSP disponíveis para *download* na Internet e aplicações diferentes para as quais RTSP é apropriado, como mídia sob demanda (Figura 6). Dentre as áreas de aplicação estão o Rádio na Internet, o controle de dispositivos, além de registro remoto, o qual é apropriado para videoconferência.

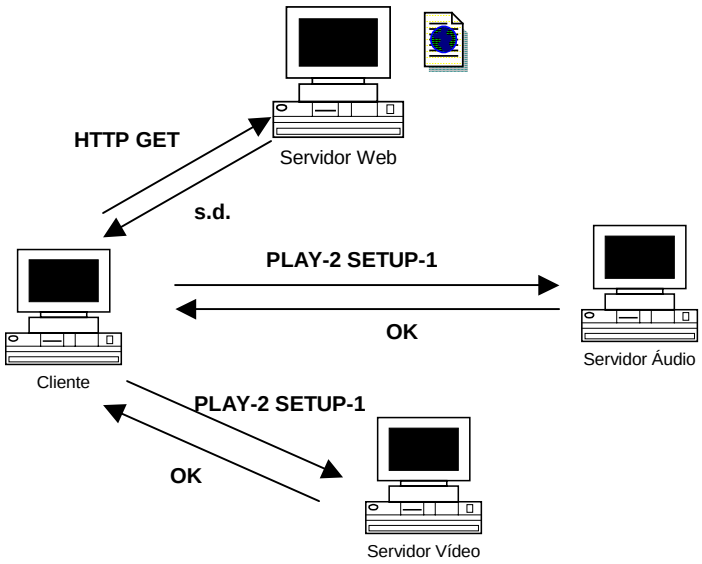

Figura 06 - Mídia sob demanda em RTSP

3.3 RealNetworks

Com mais de 130 milhões de usuários no mundo, a RealNetworks é líder no mercado de streaming media na Internet, tendo sido a empresa pioneira nestas soluções de Streaming Media (transmissão de áudio, vídeo e multimidia pela web), introduzindo as tecnologias de RealAudio, RealVideo, RealFlash, RealPix e RealText.

Para isso, ela criou uma solução que envolve uma série de aplicativos. Alguns deles rodando no Servidor e outros no Cliente. Basicamente, a RealNetworks desenvolveu três aplicativos responsáveis pela composição, distribuição e reprodução de conteúdo multimídia. São eles:

- RealProducer;
- RealServer;
- RealPlayer

Cada um deles possui suas variações, versões e subdesignações, dependendo do propósito ou finalidade em que serão empregados.

3.3.1 RealProducer

O RealProducer é responsável pela produção do conteúdo multimídia, ou seja, ele controla a captura e digitalização do áudio e do vídeo destinados a distribuição. Ele roda em ambientes Windows, Macintosh ou Unix (para plataformas Intel). Para cada tipo de aplicação, o RealProducer tem a necessidade de uma plataforma com diferente poder de processamento. Sendo assim, para a função de distribuição de vídeo sob demanda, ele necessita de menor performance, quando comparado a função de compressão e distribuição em tempo real.

O RealProducer Plus G2 elabora e transmite multimídia pela porta 4040 (padrão) sob velocidades de recepção distintas conforme sua tela principal. O áudio e vídeo elaborados são oriundos de dispositivos de captura apropriados (placas de som e/ou placas de captura de vídeo). Pode-se armazenar localmente toda a transmissão efetuada. Porém, é muito importante considerar, neste momento, aspectos de performance e capacidade de armazenamento local (espaço em disco).

Na forma de transmissão de Live Broadcast para difusão de áudio e vídeo ao vivo; pode-se, se necessário, utilizar um arquivo localizado no winchester ou dispositivo de captura como fonte de multimídia O Producer elabora conteúdo para distribuição com a criação de um arquivo .RM, que será referência para o cliente RealPlayer.

Pode-se definir larguras de banda que o servidor de áudio e vídeo pode trabalhar. Estas larguras dão liberdade de conexão com clientes a velocidades distintas, sem perder a qualidade de transmissão em demasia. É possível configurar outras opções secundárias, como títulos, autor, copyright e características da mídia a transmitir.

O interessante deste sistema de distribuição de multimídia é que o RealProducer Plus G2 não precisa estar rodando na mesma máquina que o servidor de multimídia (RealServer G2). Logo, é fácil perceber que o RealProducer não trabalha sozinho no sistema de tráfego de multimídia proposto pela RealNetworks.

3.3.2 RealServer

O RealSever é responsável pela distribuição aos clientes remotos daquilo que foi produzido no Producer (seja para transmissão em tempo real ou sob demanda). O RealServer G2 tem a função de receber o conteúdo de multimídia produzido pelo Producer e distribui-lo na rede. É possível realizar todo um gerenciamento das configurações atribuídas ao RealServer através de utilitários em Java e HTML. Essas ferramentas desenvolvidas em Java e HTML podem ser acessados via browser numa porta local, onde roda um pequeno servidor Web da própria RealNetworks destinado a esta função.

Através deste gerenciamento, é possível configurar as portas de cada protocolo (PNA, HTTP, RTSP), o processo de Logging, os diretórios HTTP existentes, o endereçamento IP a ser utilizado pelo RealServer, a porta, diretório e autenticação de acesso dos clientes, normas de segurança e muitas outras funções. É possível igualmente, acessar relatórios e menus de ajuda sobre o Real Server.

Os clientes localizados remotamente acessam o RealServer através de um número IP (ou nome do HOST), como por exemplo http://200.214.186.132 onde através de um link neste site é possível executar um conteúdo de multimídia remoto.

3.3.3 RealPlayer

No RealPlayer rtsp://200.214.186.132/encoder/.rm o número IP ou nome de HOST são referentes ao servidor de multimídia, seguido da porta de streaming RTSP previamente definida como 554 (padrão), e finalmente o diretório localizado no Producer (estrutura de pastas virtuais mantidas por ele) seguido do nome do arquivo desejado.

Para isso, o cliente RealPlayer G2, acessa um endereço determinado e começa a baixar a informação. Nos primeiros segundos, o RealPlayer armazena em um buffer local uma porção do arquivo streaming que está sendo acessado no servidor de multimídia da RealNetworks. Desta forma, ele poderá balancear a reprodução em eventuais congestionamentos da rede que comprometam a velocidade de transmissão. A transmissão de streaming de multimídia pode eventualmente sofrer variações de velocidade. Retardos de poucos segundos, no entanto, não são percebidos pela ação do buffer.

3.4 Transmissão Multimídia

Existem três formas de transmissão de multimídia através de servidores e clientes Real. A primeira é transmissão *unicast* de multimídia. A segunda forma pode ser classificada como uma transmissão *multicast* simples numa rede IP, e a terceira forma pode ser classificada como uma transmissão *multicast* confiável numa rede IP. Para efetuar a transmissão de multimídia numa destas formas ou estruturas de conexão numa rede IP, as ferramentas da Real utilizam os seguintes protocolos de comunicação:

- PNA: protocolo utilizado em versões anteriores e já em extinção;
- RTSP: Real Time Streaming Protocol (RFC 2326) é uma especificação da IETF para controle de transmissão de multimídia na Internet. Foi submetido a IETF em outubro de 1996 pela RealNetworks e pela Netscape Communications Corporation;
- IGMP: protocolo para gerenciamento de grupos de clientes em transmissões *multicast*;
- DVMRP: protocolo de roteamento em transmissões *multicast*;
- UDP/TCP: protocolos para transporte de dados;
- HTTP: protocolo utilizado, no caso das ferramentas da RealNetworks, para transmissões através de *firewalls*;

Os produtos da RealNetworks são compatíveis com padrões de arquivos de vídeo e áudio do mercado, como MPEG, AVI, WAV, VIVO, entre outros, os quais podem ser reproduzidos em seu formato original ou convertidos para um dos formatos nativos RealAudio, RealVideo, RealFlash, RealPix e RealText, a fim de alcançarem melhores taxas de transmissão.

A RealNetworks busca manter uma alta qualidade de áudio e vídeo em suas transmissões de multimídia para usuários conectados em qualquer velocidade

utilizando a compressão Dolby Labs AC3, que disponibiliza áudio estéreo em bandas de 28,8Kbps e áudio com qualidade de CD sobre ISDN ou redes locais.

A Real também oferece a opção de se desenvolver uma transmissão com bilhetagem. Para isso, a empresa oferece uma solução onde cada cliente RealPlayer possui um número identificador único (ID) que pode ser associado a um usuário ou máquina. A solução da RealNetworks é compatível com o *Synchronized Multimedia Integration Language* (SMIL), o qual compõe uma especificação do *World Wide Web Consortium* (W3C), que permite controle sobre apresentações multimídia. O SMIL descreve a sincronização das informações de mídia que aparecem na tela, a fim de que seja possível uma reprodução fiel e de qualidade. Trata-se de um controle de layout dentro do conteúdo de streaming.

3.5 Conclusão

O RTSP é um protocolo em nível de aplicação para controle na transferência de dados com propriedades de tempo real. RTSP tornando possível a transferência, sob demanda, de dados em tempo real como áudio e vídeo. Ele serve para estabelecer e controlar um único ou vários *streams* sincronizados de mídias contínuas pertencentes a uma apresentação. Este protocolo é utilizado pelo RealPlayer para transmitir os *streams* de vídeo e áudio.

Capítulo 4 – Utilizando o NTop

4.1 Introdução

Neste capítulo serão apresentados alguns exemplos de funcionamento do NTop. Estes exemplos foram retirados de uma análise feita em uma rede local com três estações, sendo que duas estações estavam com o sistema operacional Windows 98 e a outra estação com o Linux.

4.2 Estudo dos Exemplos

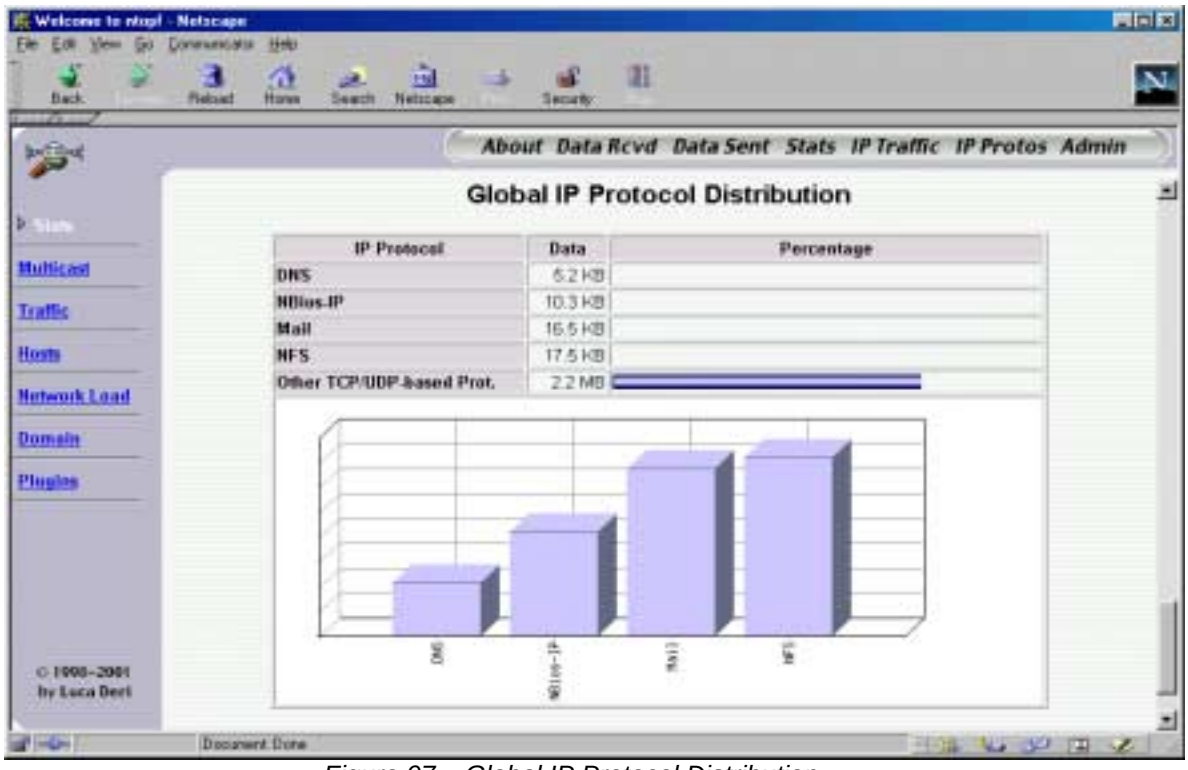

Figura 07 – Global IP Protocol Distribution

As estatísticas de tráfego relatam uma informação geral sobre o tráfego observado. O tráfego é considerado uma perspectiva global, sem informação sobre uma estação específica. Na Figura 07, é possível visualizar a tabela e o gráfico do *Global IP Protocol Distribution*. Os dados coletados pelo NTop informam que outros protocolos baseados em TCP/UDP são os protocolos que mais consomem largura de banda na rede. Este tipo de estatística é importante para o administrador entender o tráfego, associando-o com as aplicações específicas. Deste modo, é possível gerenciar a largura de banda disponível apropriadamente.

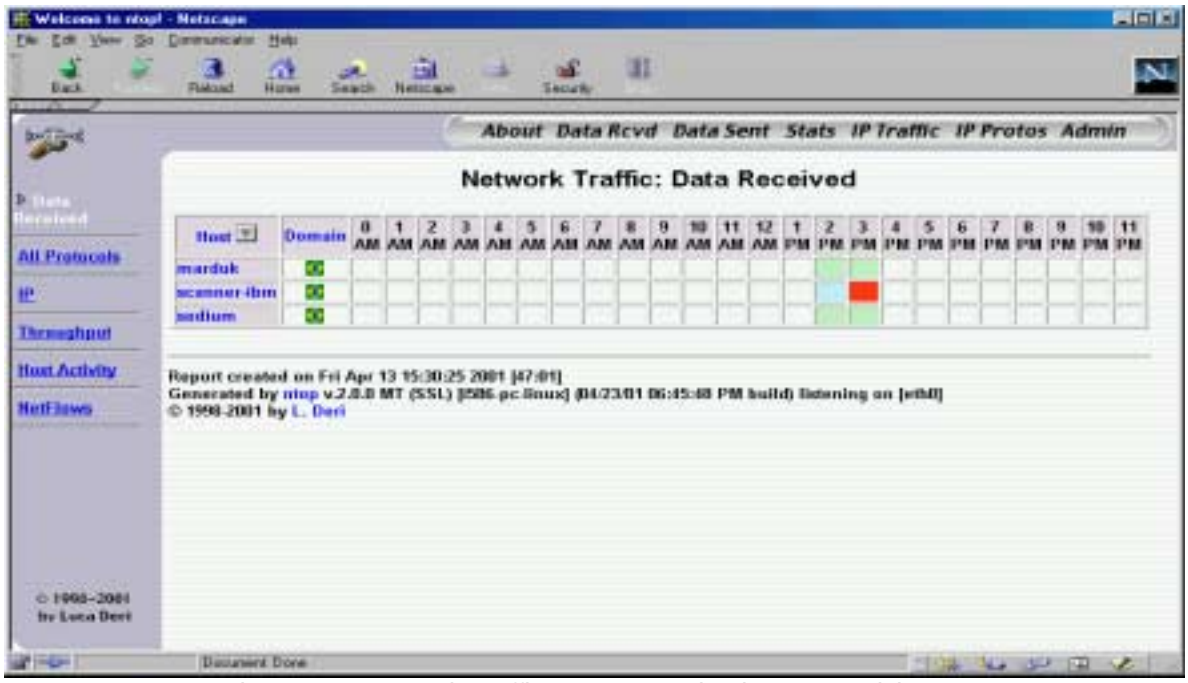

Figura 08 – Network Traffic – Data Received – Host Activity

A tabela na Figura 08 exibe o total de tráfego da rede de cada estação no tempo de 24 horas. Cada célula corresponde à uma hora específica, a cor da célula indica como o tráfego se comportou naquela hora, se a cor ficar mais intensa, isto indica que o tráfego da rede naquela hora estava sobrecarregado. Pode-se observar na Figura 6 que somente foram coletados dados às 2 e 3 horas da tarde.

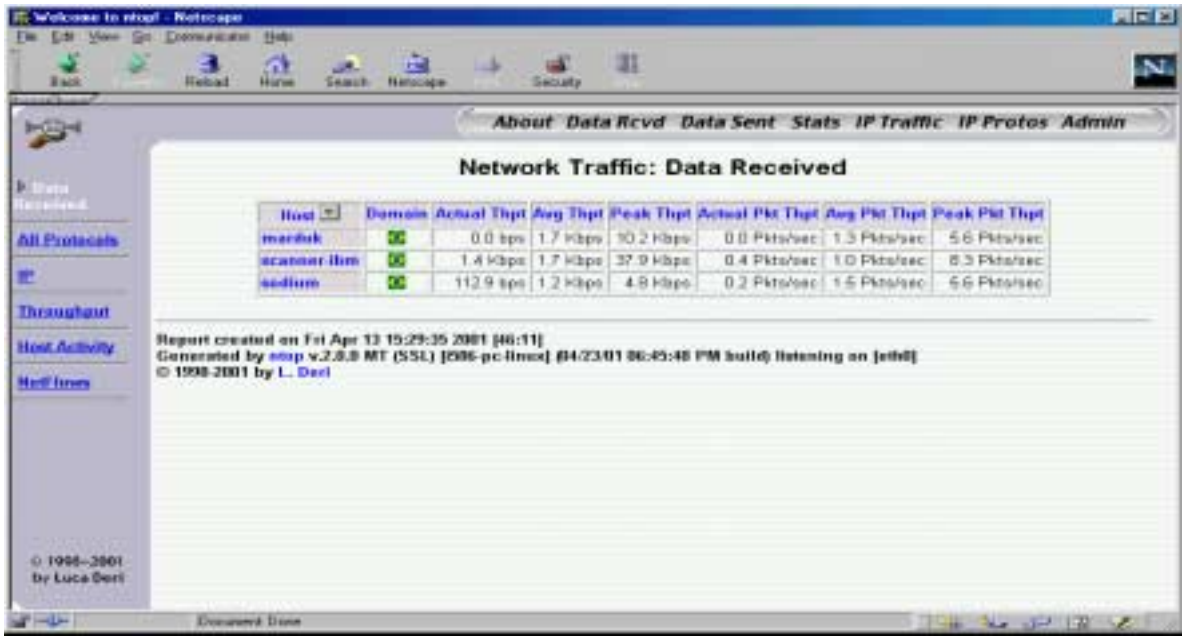

Figura 09 – Network Traffic – Data Received – Throughput

A tabela na Figura 09 exibe a vazão de cada estação que está na rede. As informações de vazão são: atual, média, máxima, atual de pacotes, média de pacotes e máxima de pacotes. A vazão atual é calculada a partir dos últimos 3 segundos, e a vazão média é calculada a partir do momento no qual o NTop é inicializado.

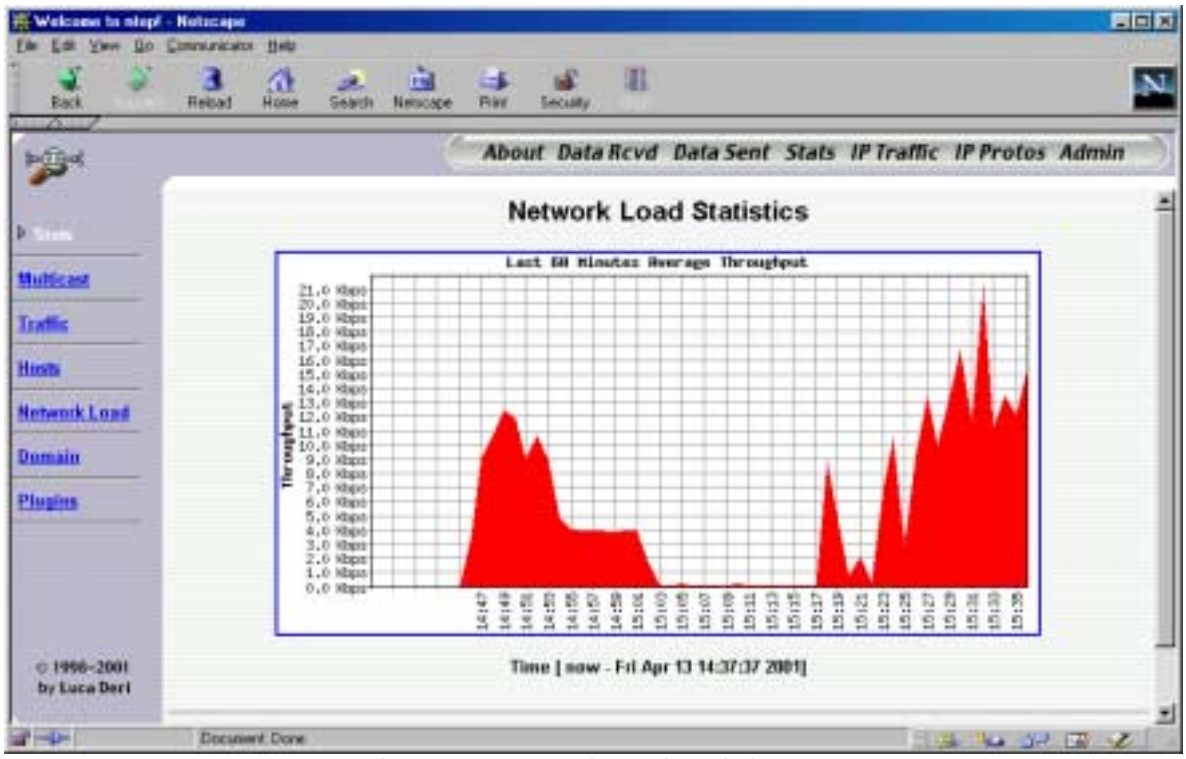

Figura 10 – Network Load Statistics

A Figura 10 exibe outra estatística de tráfego global, os gráficos de vazão. Estes gráficos mostram o andamento do total de vazão observada na rede. Eles são apresentados em diferentes escalas de tempo, mostrando a vazão dos últimos 60 minutos (mostrada acima) e das últimas 24 horas. Este tipo de estatística é importante para determinar o período mínimo e máximo de utilização. Deste modo, o administrador será capaz de estipular quando será possível executar alguns serviços, como por exemplo, manutenção física na rede, configurar o comutador, entre outros. Este tipo de informação é importante para detectar uma possível vazão máxima inesperada na rede, a qual indicaria a utilização excessiva de recursos da rede por um usuário ou grupo de usuários, ou um comportamento fora do habitual.

4.3 Conclusão

O NTop no modo *web* permite o acesso a várias informações sobre a rede que serão citadas a seguir: dados enviados, dados recebidos, estatísticas de tráfego, informação sobre uma determinada estação, protocolos IP e tráfego IP. Em cada um destes tópicos de informação sobre o tráfego existem tipos de informações detalhadas sobre um determinado tópico.

Capítulo 5 – Adicionando o Protocolo RTSP no NTop

5.1 Introdução

Neste capítulo será descrito como foi feita a inclusão do protocolo RTSP no NTop.

5.2 Registrando o RTSP

No sistema operacional Linux as informações sobre os serviços estão armazenadas no arquivo /etc/services. Este arquivo raramente precisará ser alterado, e especifica as portas de conexão de todos os serviços TCP e UDP. Ao instalar o Linux, este arquivo é criado automaticamente.

Programa: main.c

```
...
initIPServices();
...
```

A função *initIPServices()* é chamada pelo programa principal *main.c*.

Programa: initialize.c

```
...
void initIPServices(void) {
...
// Lê o arquivo services
// Adiciona os protocolos em seus respectivos registros
...
/* Add some basic services, just in case they are not included
in /etc/services */
...
  addPortHashEntry(tcpSvc, 554, "rtsp");
  addPortHashEntry(udpSvc, 554, "rtsp");
...
```

A função *initIPServices* lê o arquivo services varrendo cada linha e adicionando cada protocolo nos registros tcpSvc e/ou udpSvc. Caso o protocolo não esteja registrado no arquivo services, então será necessário acrescentá-lo. As seguintes linhas foram acrescentadas para que o protocolo RTSP seja registrado para a coleta de dados.

```
addPortHashEntry(tcpSvc, 554, "rtsp");
addPortHashEntry(udpSvc, 554, "rtsp");
```

A função *addPortHashEntry* é chamada com os seguintes parâmetros, o tipo do registro, a porta e o protocolo.

Programa util.c

```
...
void addPortHashEntry(ServiceEntry **theSvc, int port, char*
name) {
   ...
```

```
  /* Adiciona o protocolo caso ele não esteja especificado no
arquivo services */
   ...
}
...
```

Na função *addPortHashEntry* é verificado se o protocolo já está armazenado no seu determinado registro ou não. Caso o protocolo já esteja armazenado nada acontecerá, senão será feito o armazenamento.

5.3 Armazenando os dados do RTSP

Programa: main.c

```
...
time_t lastTime;
...
postCommandLineArgumentsInitialization(&lastTime);
...
```

No programa main.c a variável *lastTime* indica a hora inicial de execução do NTop. A partir desta hora será calculado tempo de *refresh* da página e o tempo de intervalo para exibição da analise dos dados na saída do terminal.

Programa initialize.c

```
...
void postCommandLineArgumentsInitialization(time_t *lastTime
_UNUSED_) {
...
  if(numIpProtosToMonitor == 0)
    addDefaultProtocols();
...
}
...
```

A função *postCommandLineArgumentsInitialization* verifica se existe algum protocolo à ser monitorado, caso não exista será chamada a função addDefaultProtocols().

Programa: ntop.c

```
...
void addDefaultProtocols(void) {
  ...
  handleProtocolList("HTTP", "http|www|https|");
  ...
  /* 554 == rtsp */
  handleProtocolList("RTSP", "554|");
  ...
}
...
```

Na função *addDefaultProtocols* é especificado os serviços do protocolo que utiliza o TCP/UDP para transporte, no caso do RTSP somente é incluída a porta. O

protocolo HTTP têm três serviços disponíveis que são: http,www e https; neste caso estes serviços são especificados.

Programa: ntop.c
```
static void handleProtocolList(char *protoName, char
*protocolList) {
 ...
// Separa os serviços/portas a serem monitorados
...
rc = handleProtocol(protoName, lastEntry);
...
}
```

Na função *handleProtocolList* são separados os serviços/portas a serem monitorados e cada um deles é enviado para a função *handleProtocol* que irá ativar o serviço.

Programa: ntop.c
```
static short handleProtocol(char* protoName, char *protocol) {
 ...

 /* Recebe-se cada serviço com o nome do protocolo */
 ...

 /* Estipula-se o valor mínimo e máximo das portas a serem
analisadas */
 ...
 if((udpSvc[i] != NULL) && (strcmp(udpSvc[i]->name, protocol) ==
0))

 /* É verificado se o protocolo já está registrado, atualizando
o número de portas a serem analisadas */
  idx = udpSvc[i]->port;
else if((tcpSvc[i] != NULL) && (strcmp(tcpSvc[i]->name,
protocol) == 0))

// verifica se o protocolo já está registrado, atualizando o
número de portas a serem analisadas
      idx = tcpSvc[i]->port;
...
 }
```

A função *handleProtocol* recebe cada serviço/porta com o protocolo, com esse dado é estipulado o valor mínimo e máximo das portas a serem analisadas. Após isso é verificado se este protocolo está registrado, se for encontrado então será atualizado o número de portas a serem analisadas. Caso o protocolo não esteja especificado no arquivo *services* e não tenha sido acrescentado com foi descrito no item 5.2 deste capítulo, nada será feito.

5.4 Adicionando o RTSP à Página Web

Programa: main.c
```
...
initWeb(webPort, webAddr, sslAddr);
...
```

No programa *main.c* é chamada a função *initWeb* que é responsável pela inicialização do página *web* do monitoramento do NTop.

Programa webInterface.c

```
...
void initWeb(int webPort, char* webAddr, char* sslAddr) {
...
createThread(&handleWebConnectionsThreadId,
handleWebConnections, NULL);
...
}
...
```

A função *initWeb* verifica qual o modo HTTP será utilizado e verifica se a porta escolhida está sendo utilizado por outro aplicativo.

Programa webInterface.c

```
...
void* handleWebConnections(void* notUsed _UNUSED_) {
...
handleSingleWebConnection(&mask);
...
}
...
```

Na função *handleWebConnections* é estabelecida as conexões com a página.

Programa webInterface.c

```
...
void handleSingleWebConnection(fd_set *fdmask) {
...
  handleHTTPrequest(from.sin_addr);
...
}
...
```

Na função *handleSingleWebConnection* é verificado o estabelecimento das conexões.

Programa http.c

```
...
void handleHTTPrequest(struct in_addr from) {
...
postLen = readHTTPheader(requestedURL, sizeof(requestedURL), pw,
sizeof(pw));
...
  if((rc = returnHTTPPage(&requestedURL[1], postLen)) == 0 ) {
...  }
...
```

A função *handleHTTPrequest* organiza a página a ser exibida.

Programa: http.c

```
...
```

```
static int readHTTPheader(char* theRequestedURL, int
theRequestedURLLen, char *thePw, int thePwLen) {
...
// retorna o cabeçalho da página
...
}
...
```

A função *readHTTPheader* gera o cabeçalho da página a ser exibido e retorna a função *handleHTTPrequest*.

Programa: http.c

```
...
static int returnHTTPPage(char* pageName, int postLen) {
...
sendString("<ul><li>TCP/UDP/ICMP<li>(R)ARP<li>IPX<li>DLC<li>"

"Decnet<li>AppleTalk<li>Netbios<li>TCP/UDP<ul><li>FTP<li>"

"HTTP<li>DNS<li>Telnet<li>SMTP/POP/IMAP<li>SNMP<li>RTSP<li>\n");
...
}
...
```

A função *returnHTTPPage* gera as páginas solicitadas. Nesta função foi acrescentado o protocolo RTSP para que os dados coletados sobre ele sejam exibidos.

5.5 Conclusão

O NTop é um software que permite alterações por ser um software de código aberto. Para acrescentar um protocolo é necessário ter algum conhecimento de como ele funciona, se todos os sistemas operacionais o utilizam e etc.

Conclusão

Neste projeto foi acrescentado ao aplicativo de monitoramento de tráfego da rede (NTop) uma análise do Real Time Streaming Protocol (RTSP). O protocolo RTSP é utilizado pelas mídias de áudio e vídeo do RealPlayer da empresa RealNetworks. O sistema operacional Linux é utilizado para rodar o NTop, como também para a modificação e teste. O NTop (Network Top) é um aplicativo gratuito que permite o monitoramento da atividade da rede.

O administrador da rede, com o NTop, tem o controle de como a sua rede se comporta, podendo analisar futuramente uma ampliação da mesma, caso apareça algum saturamento da rede. O NTop permite ao administrador analisar detalhadamente uma máquina e observar quais os protocolos que ela utiliza e outras informações. Como podemos observar o NTop tem características que são relevantes como: servidor HTTP embutido, suporte a vários tipos de enlaces de rede, pouca utilização da CPU, portabilidade para várias plataformas, armazenamento das informações de tráfego em um banco de dados SQL, e integração com várias ferramentas de rede.

O desempenho do NTop é influenciado pelos outros processos correntes, porque algumas aplicações "gananciosas" de CPU podem utilizar todos os ciclos da CPU durante alguns segundos causando perda de pacotes. Se a rede tem muito fluxo de dados, o desempenho do NTop é comprometido, pois ele terá que analisar muitos pacotes. O NTop somente analisa o segmento de rede no qual a estação ntop está. Se mais de um segmento de rede estiver que ser analisado, uma estação em cada segmento de rede deverá ter o NTop instalado.

Futuramente o NTop poderá ser utilizado para monitorar uma parte do tráfego da Rede Rio, permitindo analisarmos o crescimento do volume de tráfego de Internet nesta rede. Na rede local do CBPF será utilizado para monitorarmos os dados de entrada e saída do CBPF, para um conhecimento maior dos tipos de dados que trafegam nesta rede.

O NTop é um aplicativo que controla o tráfego disponibilizando dados sobre os protocolos mais utilizados na rede. O NTop tem o seu código-fonte aberto e é um aplicativo gratuito, permitindo aos seus usuários modificá-lo de acordo com a sua necessidade adequando-o a sua rede, sendo ele projetado na linguagem C. Tendo o NTop estas características foi permitido a alteração no código-fonte para acrescentar o protocolo RTSP. Poderiam ser feitas outras modificações no NTop para que cada vez mais ele seja um aplicativo completo de monitoramento de tráfego da rede.

Referências Bibliográficas

1. JACOBSON V., MCCANNE S., 1993, “The BSD Packet Filter: A New Architecture for User-level Packet Capture”, *Proc. of 1993 Winter USENIX Conference*.
2. ETHERAPE. Disponível na World Wide Web: <http://etherape.sourceforge.net>.
3. ETHEREAL. Disponível na World Wide Web: <http://www.ethereal.com>.
4. FREE SOFTWARE FOUNDATION, 1999, GNU gdbm. Disponível na World Wide Web: <http://www.gnu.org/software/gdbm/gdbm.html >.
5. IPTRAF. Disponível na World Wide Web: <http://cebu.mozcom.com/riker/iptraf>.
6. KNETDUMP. Disponível na World Wide Web: <http://www.knetdump.de/>.
7. KSNIFFER. Disponível na World Wide Web: <http://ksniffer.veracity.nu/>.
8. KSNUFFLE. Disponível na World Wide Web: <http://www.quaking.demon.co.uk/ksnuffle.html>.
9. LSOF. Disponível na World Wide Web: <http://www-rcd.cc.purdue.edu/~abe/>.
10. NDIS. Disponível na World Wide Web: <http://www.microsoft.com/hwdev/devdes/ndis5.htm>.
11. NTOP. Disponível na World Wide Web: <http://www.ntop.org>.
12. REALNETWORKS. Disponível na World Wide Web: <http://www.realnetworks.com/>.
13. TCPDSTAT. Disponível na World Wide Web: <http://www.csl.sony.co.jp/~kjc/papers/freenix2000/node14.html>.
14. TCPDUMP. Disponível na World Wide Web: <http://www.tcpdump.org>.
15. TCPFLOW. Disponível na World Wide Web: <http://www.circlemud.org/~jelson/software/tcpflow/>.
16. TCPSLICE. Disponível na World Wide Web: <http://www.cs.ucf.edu/~allen/security/man/tcpslice8.html>.
17. TCPSTAT. Disponível na World Wide Web: <http://www.frenchfries.net/paul/tcpstat/>.
18. TCPTRACE. Disponível na World Wide Web: <http://www.tcptrace.org/>.

Glossário

ANSI (American National Standards Institute)
1. Uma organização afiliada à ISO e que é a principal organização norte-americana envolvida na definição de padrões (normas técnicas) básicos como o ASCII. 2. Conjunto de normas para a transferência de caracteres de controle. Utilizado para tratamento de atributos, cores, endereçamento do cursor, etc, em terminais ou emuladores de terminais.

Anúncios de janelas de recepção (Window advertisements)
Tamanho do buffer de recepção TCP de alguma estação. Este dado diz o quanto uma dada estação pode receber sem que haja descartes no destino naquele instante.

Aplicação
Programa que faz uso de serviços de rede tais como transferência de arquivos, *login* remoto e correio eletrônico.

Apple Talk
É um conjunto de protocolos dispostos em camadas, onde cada protocolo implementa (oferece) um conjunto de serviços utilizados pelo protocolo da camada superior (denominado de cliente).

ARP (Address Resolution Protocol)
Protocolo que resolve o endereço Ethernet do seu endereço *Internet*. O transmissor envia uma mensagem de difusão com endereço *Internet* e espera pela resposta de outro servidor que contém o endereço Ethernet correspondente. Cada servidor mantém uma *cache* com traduções de endereços *Internet* em Ethernet para reduzir a latência envolvida neste processo. O ARP permite que os endereços *Internet* sejam independentes dos endereços Ethernet, mas só funciona se todos os servidores o suportarem.

ASCII (American Standard Code for Information Interchange)
Código Padrão Americano para o Intercâmbio de Informações. Inicialmente um código de sete bits (e o oitavo bit era conhecido como bit de paridade) usado para representar 128 símbolos, incluindo todos os caracteres alfanuméricos básicos, com bits de dados; formalizado pelo Instituto Americano de Padrões, porém mais tarde aprimorado pela IBM; agora um sistema de oito bits que descreve 256 símbolos.

Backbone
Espinha dorsal. Estrutura de nível mais alto em uma rede composta por várias sub-redes. O *backbone* é composto por linhas de conexão de alta velocidade, que se conectam as linhas de menor velocidade.

Biblioteca
Coleção de funções que foram compiladas para código-objeto.

Bit (BInary digiT)
Um dado; menor unidade de informação; pode ser um 0 ou um 1.

Bit de paridade
Bit extra em um byte, usado para detectar erros; usado na versão original do conjunto ASCII.

bps (bits per second)
Uma medida da taxa de transferência real de dados de uma linha de comunicação. É dada em *bits* por segundo. Variantes ou derivativos importantes incluem Kbps (= 1000 bps) e Mbps (= 1000.000 bps)

Bridge (Ponte)
Um dispositivo que conecta duas ou mais redes de computadores transferindo, seletivamente, dados entre ambas.

Broadcast
O termo *broadcast* é usado para definir as transmissões de dados abertas, ou seja, um remetente transmitindo para todos aqueles que quiserem ou tiverem a capacidade de receber os dados. Funciona como o sistema de rádio e televisão, onde uma emissora transmite um sinal aberto, e todos com o equipamento adequado podem recebe-lo.

Buffer
Um local de armazenamento temporário de informações.

Byte
Oito bits (octeto); quantidade de memória exigida para armazenar um único caracter; unidade de dado capaz de armazenar 256 valores únicos.

Cabeçalho
São informações de controle de protocolo, tipo mensagem - carga útil.

Cache
Um subsistema especial de memória para o qual os valores dos dados utilizados com freqüência são copiados para permitir um acesso mais rápido.

Cavalo de Tróia (Trojan Horse)
São programas que ocultam os seus reais objetivos sob uma camuflagem de programas úteis ou inofensivos. Um exemplo hipotético de *trojan horse* seria um programa escrito, por exemplo, para formatar de forma incondicional o disco rígido, oferecido como um duplicador de disco ou PC game.

Compilador
Programa que traduz um arquivo de código-fonte de um programa para código-fonte de um programa para código-objeto.

Comutador (Switch)
Dispositivo eletrônico capaz de segmentar uma rede de dados em diferentes velocidades. Muito usado para redes com topologia simultânea Ethernet e *Fast* Ethernet.

Criptografia
Criptografia é a técnica de converter (cifrar) uma mensagem ou mesmo um arquivo utilizando um código secreto. Com o propósito de segurança, as informações nele contidas não podem ser utilizadas ou lidas até serem decodificadas.

DECNet
Protocolo de rede, criado pela Digital Eletronic Corporation. Tem por característica identificar os nós da rede através de um número, em que a 1a parte é o número de área, seguida por um ponto, e a 2a parte é um número seqüencial de 1 a 1024, identificador da estação. Cada estação é conhecida na rede através de um nome, que tem que ser único para toda a rede, e pelo número do nó

DLC (Data Link Protocol)
Diferentemente de outros protocolos, este protocolo não foi designado para ser o protocolo primário para a utilização na rede entre computadores pessoais. O DLC é utilizado no NT principalmente para as seguintes tarefas: acessar *mainframes* da IBM e imprimir em impressoras HP (Hewlett-Packard) que estejam diretamente conectadas a rede.

DNS (Domain Name Service)
É um serviço e protocolo da família TCP/IP para o armazenamento e consulta de informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes *Internet* em seus endereços IP correspondentes.

Estação (host)
Computador ligado a *Internet*.

Ethernet
Um padrão muito usado para a conexão física de redes locais, originalmente desenvolvido pelo PARC (Palo Alto Research Center) da Xerox nos EUA. Descreve protocolo, cabeamento, topologia e mecanismos de transmissão. Os dados trafegam a velocidade nominal de 10 Mbps.

FDDI (Fiber Distributed Data Interface)

Um padrão para o uso de cabos de fibras óticas em redes locais (LANs) e metropolitanas (MANs). A FDDI fornece especificações para a velocidade de transmissão de dados (alta, 100 Mbps), em redes em anel, podendo, por exemplo, conectar 1000 estações de trabalho a distâncias de até 200 Km.

Flag
Um caracter ou conjunto de caracteres utilizado para delimitar quadros em um esquema de multiplexação de pacotes.

Flag FIN
Quando uma das estações sinaliza a *flag* FIN para a outra significa que ele quer finalizar a conexão. Esta *flag* pertence ao protocolo TCP.

Fragmento IP
O protocolo IP realiza a fragmentação de pacotes muito grandes em pacotes menores, a fim de permitir o seu encaminhamento em redes que não suportam unidades de dados muito grandes. Estas unidades menores são denominadas fragmentos.

Framework
Um *framework* captura a funcionalidade comum a várias aplicações.

FTP (File Transfer Protocol).
Protocolo padrão de transferência de arquivos entre computadores, usado normalmente para transmitir ou receber arquivos via *Internet*.

GCC
Compilador GCC da Gnu para linguagem C/C++.

Gopher
Um sistema distribuído para busca e recuperação de documentos, que combina recursos de navegação através de coleções de documentos e bases de dados

indexadas, por meio de menus hierárquicos. O protocolo de comunicação e o software seguem o modelo cliente-servidor, permitindo que usuários em sistemas heterogêneos naveguem, pesquisem e recuperem documentos armazenados em diferentes sistemas, de maneira simples e intuitiva.

HTML (Hypertext Markup Language)
Linguagem padrão usada para escrever páginas de documentos para Web ou WWW. É uma variante da SGML (Standard Generalized Markup Language), bem mais fácil de aprender e usar, possibilitando preparar documentos com gráficos e *links* para outros documentos para visualização em sistemas que utilizam *Web*.

HTTP (HyperText Transfer Protocol)
Este protocolo é o conjunto de regras que permite a transferência de informações na *Web* e permite que os autores de páginas de hipertextos incluam comandos que possibilitem saltos para recursos e outros documentos disponíveis em sistemas remotos, de forma transparente para o usuário.

Hub
Um ponto de conexão para acessórios em uma rede. Os *hubs* são geralmente usados para conectar segmentos de uma rede local. Ele contém portas múltiplas. Quando um pacote de informações chega em uma porta, ele é copiado para as outras portas para que todos os segmentos da rede local possam ver o pacote. Alguns *hubs* podem ler o endereço de destino de cada pacote e então direcioná-lo para a porta correta.

ICMP (Internet Control Message Protocol)
Extensão do protocolo IP. Suporta pacotes de contendo mensagens de controle, informação e erro. O comando *ping*, por exemplo, utiliza esse protocolo para testar uma conexão de rede.

IMAP (Internet Message Access Protocol)
É um protocolo que permite que um utilizador execute determinadas funções de *mail* num servidor remoto a partir de um computador local.

Interface de rede
É o dispositivo que conecta o meio físico a estação.

IP (*Internet* Protocol)
É o protocolo responsável pelo roteamento de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e usada na *Internet*. é o mais importante dos protocolos em que a *Internet* é baseada.

IP Spoofing
Este ataque consiste no ganho de acesso não-autorizado a computadores de uma rede privada.

IPX

É um protocolo que utiliza datagramas, ou seja, cada pacote é tratado como uma entidade individual, não possuindo nenhuma relação lógica ou de seqüência com outros pacotes. O protocolo IPX é meio base de transferência de informação na arquitetura cliente servidor das redes NetWare. Nesta arquitetura (cliente-servidor), todas as comunicações ocorrem entre as máquinas clientes e o servidor NetWare.

ISO (International Organization for Standardization)

Uma organização internacional formada por órgãos de diversos países, tais como o ANSI (americano), o BSI (inglês), o AFNOR (francês) e a ABNT (brasileira), e que estabelece padrões industriais de aceitação mundial.

JPEG (Joint Photographic Expert Group)
Formato de arquivo utilizado para a compactação de extensos arquivos de imagens coloridas.

KDE
Interface gráfica do sistema operacional Linux.

Kernel
Parte de um sistema operacional que controla as funções centrais do computador, com o gerenciamento do hardware e da memória interna.

Largura de banda
Termo que designa a quantidade de informação passível de ser transmitida por unidade de tempo, num determinado meio de comunicação (fio, onda rádio, fibra óptica, etc.).

Links ou HiperLinks
Conexão, ou seja, elementos físicos e lógicos que interligam os computadores da rede. São ponteiros ou palavras chaves destacadas em um texto, que quando "clicadas" nos levam para o assunto desejado, mesmo que esteja em outro arquivo ou servidor.

Loopback
O objetivo do Loopback é permitir teste de comunicação inter-processos na máquina local. Quando um programa usa o endereço de loopback para enviar dados, o software do protocolo retorna o dado sem gerar tráfego na rede.

MAC ADRESS (Endereço de máquina)
É o número de identificação da placa de rede de cada computador.

Multicast
Um endereço para uma coleção especifica de nós numa rede, ou uma mensagem enviada a uma coleção especifica de nós. É útil para aplicações como teleconferência.

Multiplexação
É uma técnica que permite a transmissão de mais de um sinal em um mesmo meio físico, ou seja, é o compartilhamento de um meio de transmissão por vários usuários.

Navegador
O navegador é um cliente para extração de informação em um servidor *Web* ou *gopher*. Tipicamente, um navegador será um programa em um computador pessoal que acessará, através de uma linha telefônica, um servidor (isto é, um programa que atende a demanda de clientes remotos) contendo informações de interesse amplo.

Negação de Serviço (Denied of Service)
Um ataque de Negação de Serviço (DoS) não é um vírus, mas um método utilizado por hackers para impedir ou negar acesso de usuários legítimos a um computador. Os ataques de DoS são normalmente executados usando ferramentas de DoS que enviam muitos pacotes de solicitação a um servidor de destino pela Internet (geralmente um servidor *Web*, FTP ou Mail), sobrecarregando os recursos do servidor

e tornando o sistema inoperável. Todos sistemas conectados à Internet que esteja equipado com serviços de rede baseados em TCP estão sujeitos a ataque.

NetTBEUI (NetBIOS Extended User Interface)
Um driver de dispositivo de rede para a camada de transporte fornecido com o LAN *Manager* da Microsoft.

NetBIOS (Network Basic Input/Output System)
Sistema de Entrada e Saída da Rede. É uma camada de software (protocolo) que envia instruções para a placa de rede, permitindo que um ou mais PCS se comuniquem. É suportado por vários sistemas operacionais, sendo que às vezes o conjunto de instruções Netbios se encontram diretamente na placa de rede. Envia pela rede o nome do computador, para assegurar-se que não existam nomes de computadores/estações repetidos.

NFS (Network File System)
É o protocolo de compartilhamento de arquivos remotos, desenvolvido pela *Sun Microsystems*. Faz parte da família de protocolos TCP/IP.

Nó
Qualquer dispositivo, inclusive servidores e estações de trabalho, ligado a uma rede.

ODBC (Open DataBase Connection)
É uma ferramenta também utilizada pelo Access para conectar-se a outros tipos de bancos de dados, como dBase, FoxPro, Paradox e até Access.

OSI (Open Systems Interconnection)
É um modelo conceitual de protocolo com sete camadas, definido pela ISO, para a compreensão e o projeto de redes de computadores. Trata-se de uma padronização internacional para facilitar a comunicação entre computadores de diferentes fabricantes.

Pacote
Dado encapsulado para transmissão na rede. Um conjunto de bits compreendendo informação de controle, endereço fonte e destino dos nos envolvidos na transmissão.

Pilha TCP/IP
É uma pilha de protocolos que inclui diversos protocolos, dos quais o TCP e o IP são os mais importantes. Essa pilha é dividida em quatro camadas principais: Aplicações, Transporte, Rede e Enlace, além da camada Física, que é composta pelas placas de interface de rede e o meio físico de comunicação.

Ping (Packet *Internet* Group)
O *ping* é um programa TCP/IP usado para testar o alcance de uma rede, enviando a nós remotos uma requisição e esperando por uma resposta.

Plataforma
É o tipo de computador, processador, sistema operacional em uso. Ex.: Este programa funciona somente em plataforma IBM-PC ou funciona em plataforma Macintosh, RISC.

Plug-Ins
Extensões do navegador, fornecidas pelo fabricante do navegador ou empresas parceiras que fornecem recursos adicionais de multimídia, facilitando a visualização de textos, som, vídeo, etc. e maior interação com o usuário.

PNG
Similar ao GIF, é suportado pelos dois principais navegadores, Internet Explorer e Netscape Navigator. Sua diferença básica em relação ao GIF é que este se baseia numa tecnologia patenteada pela Unisys.

POP (Point-of-Presence / Post Office Protocol)
1. Em português Ponto-de-Presença (PP);
2. Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

Porta
Uma abstração usada pela *Internet* para distinguir entre conexões simultâneas múltiplas para uma única estação destino. O termo também é usado para denominar um canal físico de entrada e saída de um dispositivo.

Portscan
É o processo de conexão em diversas portas TCP / UDP (Geralmente em uma seqüência (1, 2, 3, 2000, 2001...) com o intuito de identificar quais portas estão em 'LISTENING STATE', ou seja, aptas para receber uma conexão. Deste modo é possível identificar alguns dados sobre o sistema, assim como serviços (TCP/UDP) que o mesmo executa, sistema operacional, etc.

PP (Ponto de Presença)
Local na espinha dorsal de rede, onde uma rede permite acesso à sub-redes e a provedores de serviços. Uma rede madura cobre sua região de atuação através de pontos-de-presença nas principais cidades/distritos dessa região: interligados por um conjunto de linhas dedicadas, compondo um backbone.

PPP (Point-to-Point Protocol)
Um dos protocolos mais conhecidos para acesso via interface serial. O PPP estabelece um método de acesso a *Internet* em que um computador, ligado a uma estação *Internet* via telefone e um modem de alta velocidade, aparece para a estação como se fosse uma porta Ethernet no sistema de rede local da estação.

Protocolo
Um conjunto de regras padronizado que especifica o formato, a sincronização, o seqüenciamento e a verificação de erros em comunicação de dados. Uma descrição formal de formatos de mensagem e das regras que dois computadores devem obedecer ao trocar mensagens. O protocolo básico utilizado na *Internet* é o TCP/IP.

Proxy
Programa que permite a comunicação entre duas redes, efetuando ou não processamento adicional.

RARP (Reverse Address Resolution Protocol)
De forma inversa ao ARP, o RARP procura um endereço IP relacionado a um endereço físico determinado. Geralmente quem mais utiliza tal protocolo são as estações de rede sem disco que possuem apenas o endereço físico, durante o processo de inicialização.

Raw IP
Envio de dados encapsulados diretamente em datagramas IP, sem passar pelo nível de transporte, diretamente da aplicação.

RNP (Rede Nacional de Pesquisa)
A RNP conecta redes de pesquisa e educação em todo o Brasil. *www.rnp.br*.

Roteador
Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes. Tipicamente, uma instituição, ao se conectar a *Internet*, deverá adquirir um roteador para conectar sua Rede Local (LAN) ao Ponto-de-Presença mais próximo. Roteadores vivem se falando aos pares, como *modems.*

SMTP (Simple Mail Transfer Protocol)
Protocolo *Internet* usado para correio eletrônico.

SNMP (Simple Network Management Protocol)
Protocolo usado para monitorar e controlar serviços e dispositivos de uma rede TCP/IP. É o padrão adotado pela RNP para a gerência de sua rede.

Sockets
Conectores utilizados entre as aplicações e rede.

SQL (Structured Query Language)
Linguagem padrão de consulta usada para procurar e selecionar registros e campos em uma tabela de banco de dados.

TCP/IP (Transmission Control Protocol/*Internet* Protocol)
Família de protocolos que torna possível a comunicação de computadores de redes diferentes. É um padrão de fato para inter-redes abertas e a linguagem universal da *Internet*.

Telnet
Uma das aplicações da *Internet*, que permite o *login* remoto, tornando possível a um microcomputador atuar como terminal de computadores de qualquer parte do mundo. O *Telnet* atua no modo texto e permite usar um computador, que está longe, como se fosse o seu próprio micro.

Token Ring
Protocolo comum de rede local baseado na topologia de anel, em que computadores ligados compartilham uma ficha para facilitar a passagem dos dados.

Topologia
É a forma como as estações de trabalho estão dispostas relativamente umas às outras e/ou a um computador central.

Traceroute
O *traceroute* é uma ferramenta que permite descobrir o caminho feito pelos pacotes desde a sua origem até o seu destino.

Unicast
Tecnologia que permite o envio de pacotes de uma máquina diretamente a outra.

UDP (User Datagram Protocol)
Protocolo de transporte sem conexão da família TCP/IP, usado com aplicações como o de gerenciamento de redes (SNMP) e de serviço de nomes (DNS).

URL (Uniform Resource Locator)
Código para localização universal, que permite identificar e acessar um serviço na rede *web*.

Vazão (Throughput)
Uma medida da quantidade de dados (ou de volume) emitidos em uma quantidade de tempo dada. Por exemplo, a videoconferência pode requerer 384 Kbps a fim de fornecer a qualidade satisfatória. Descarregar uma página de texto de um servidor web em dois segundos requer uma vazão de 20 Kbps.

X11
Protocolo de acesso a aplicações gráficas em sistemas UNIX.

XML (eXtended Markup Language)
Linguagem de descrição de páginas extensível e personalizável, que pretende colocar um fim nos problemas de dialetos incompatíveis de HTML.

WAP (Wireless Aplication Protocol ou Protocolo para aplicações sem fio)
O WAP foi projetado para realizar de forma fácil e inovadora, aplicações de comunicação de dados sem fio na Web.

Web ou WWW ou W3 (World Wide Web)
Literalmente, teia de alcance mundial. Baseada em hipertextos, integra diversos serviços *Internet* que oferecem acesso, através de *hiperlinks*, a recursos multimídia da *Internet*. Responsável pela popularização da rede, que agora pode ser acessada através de interfaces gráficas de uso intuitivo, como o Netscape ou Mosaic, a *Web* possibilita uma navegação mais fácil pela *Internet*.